REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Drawings

Applicant respectfully requests that the Examiner indicate whether the drawings submitted on September 17, 2001, are acceptable.

Disposition of Claims

Claims 1, 2, and 4-9 are pending in the present application. Claim 1 is independent. The remaining claims depend, directly or indirectly, from claim 1.

Title Amendments

The title has been amended to be clearly indicative of the invention to which the claims are directed.

Claim Amendments

Independent claim 1 has been amended to clarify the invention. Specifically, the preamble of claim 1 has been amended to clarify: (i) that a first module is onboard an administration server, (ii) at least one second module is onboard a public payphone terminal, and (iii) that the first module includes at least one file of secret data associated with at least a type of user card which is used in connection with said second module. Further, claim 1 has been amended to correct an antecedent basis error. Specifically, claim 1 now requires that information including the random data item stored in the first memory of the second module is

transferred from the first memory to the *second* memory of the second module. Support for the aforementioned amendments may be found, for example, on page 5, lines 16-22, page 6, lines 6-13, and page 7, lines 19-23 of the Instant Specification. Further, claims 2-9 have been amended to correct minor errors. No new matter has been added by any of the aforementioned amendments.

Specification Amendments

The Applicant has amended the abstract to address the concerns raised by the Examiner in the Office Action mailed July 20, 2005. No new matter has been added by these amendments.

Rejection(s) under 35 U.S.C. § 112

Claims 1, 2, and 4-9 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Claim 1 has been amended in this reply to clarify the invention recited. Specifically, claim 1 has been amended to clarify that information is transferred to the *second* memory of the second module. Accordingly, claims 1, 2, and 4-9 are no longer indefinite, and withdrawal of this rejection is respectfully requested.

Rejection(s) under 35 U.S.C. § 102

Claims 1, 2, and 4-9 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,067,921 issued to Yu et al. (hereinafter "Yu"). For the reasons set forth below, this rejection is respectfully traversed.

The invention, as recited in the amended claims, is directed to a method for loading data from a first module on an administration server to a second module on a public payphone terminal. As recited in the amended claims, a random number is initially transferred from a second module residing on the public payphone to a first module residing on the administrative server. The random number is then used to encrypt secret data on the first module. Once the secret data is encrypted, the secret data is transferred from the first module to the second module (*see* Specification, page 5, line 13 – page 6, line 5).

Yu does not disclose the above transmission of information between a first module and a second module as recited in the pending claims. Rather, Yu is directed to authenticating a user using an IC card **100** at a terminal **120** with a one-time password (*see* Yu, abstract).

Specifically, Yu discloses using a particular algorithm to generate a one-time password with the terminal **120** and using the same algorithm to generate a one-time password within a server **140** (*see* Yu, col. 6, lines 34-39, col. 7, lines 27-35). The one-time password generated at the terminal **120** is subsequently communicated to the server **140** (*see* Yu, col. 8, lines 1-9). Once the server **140** receives the one-time password from the terminal **120**, the server **140** compares the one-time passwords to determine whether the one-time password generated in the terminal **120** is the same as the password generated in the server **140** (*see* Yu, col. 8, lines 10-17). If the passwords match, the user of the IC card **100** is authenticated (*see* Yu, col. 8, lines 61-67).

As discussed above, the one-time passwords are generated with a specific algorithm that uses a random number and a secret key, where the secret key is stored in the IC card **100** of the terminal **120**. At the terminal **120**, the random number is generated in the IC card **100** and subsequently transferred, along with the one-time password, to the server **140** (*see* Yu, col. 8,

lines 1-17). Upon receipt of the random number and the one-time password, the server **140** generates the one-time password using the random number.

The Examiner asserts that Yu discloses, within the first module, encrypting a secret data item in the file of the first module based on the random data item and an encryption algorithm, sending the encrypted secret data item to the second module (*see* Office Action of July 20, 2005, page 4). However, from the above discussion, it is clear that Yu merely discloses the generation of a one-time password using the random number in the server **140** (*see* Yu, col. 7, lines 40-43) and the reception (in the server **140**) of the random number and a one-time password from the terminal **120** (*see* Yu, col. 8, lines 1-9).

In other words, Yu discloses passing two separate and distinct items *from the terminal **120** to the server **140***: (i) a random number from the terminal **120** to the server **140** for generation of a password in the server **140** and (ii) the password from the terminal **120** to the server **140** for authentication in the server **140**. However, Yu does not teach or suggest bi-directional communication as recited in the claims. In particular, Yu does not disclose communicating a random number from the second module to the first module and then transferring encrypted secret data from the first module to the second module, where the secret data is encrypted using the random number. In view of the above, it is clear that Yu does not disclose the direction (*i.e.,* where does the communication originate and terminate) and content of the communication (*i.e.,* what is passed between the first module and the second module) as required by amended independent claim 1.

Further, Yu explicitly discloses deleting the random number from the IC card **100** (*see* Yu, col. 6, lines 40-46). This is in clear contrast to the claims. In particular, the claims require that the random data is stored within the first memory of the second module. Because the random number is used to decipher secret data that is sent from the first module to the second

module, the random number must necessarily be saved in the second module in order for enable the second module to decrypt the encrypted secret data.

In addition to failing to teach or suggest the above limitations of claim 1, Yu fails to disclose "at least one second module onboard a public payphone terminal," and the first module including "at least one file of secret data associated with at least a type of user card which is used in connection with said second module," as recited in amended independent claim 1. In fact, Yu is silent with respect public payphone terminals. The Applicant does note that the aforementioned limitations are recited in the preamble of amended independent claim 1. However, the MPEP §2111.02 states that, "any terminology in the preamble that limits the structure of the claimed invention must be treated as a claim limitation." See, e.g., *Corning Glass Works v. Sumitomo Elec U.S.A., Inc.*, 868 F.2d 1251, 1257, 9 USPQ2d 1962 (Fed. Cir. 1989). The cited case indicates that the determination of whether preamble recitations are structural limitations can be resolved only in view of the application in its entirety.

The invention, as recited in the claims, is clearly directed to the problem of transferring secret data to public payphones (*see, e.g.*, Specification, page 1, lines 5-18). Because the preamble provides structure for the claims, which is clearly supported by the specification, the Examiner should appropriately consider the structure recited in the preamble as a limitation of the claims. In doing so, Yu must disclose at least one second module onboard a public payphone terminal and a first module including at least one file of secret data associated with at least a type of user card which is used in connection with the second module, as recited in amended independent claim 1. As discussed above, Yu is silent with respect to such a payphone system, and, thus, fails to teach or suggest all the limitations recited in the amended claims.

In view of the above, Yu fails to show or suggest the invention as recited in amended independent claim 1. Thus, amended independent claim 1 is patentable over Yu. Claims 2 and 4-9, directly or indirectly dependent from claim 1, are patentable over Yu for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 09669/010001).

Dated: October 20, 2005

Respectfully submitted,

By _____

Jonathan P. Osha
Registration No.: 33,986
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant

120909_2